Ollscoil na hÉireann, Gaillimh GX_____
National University of Ireland, Galway

Summer Examinations, 2009

Exam Code(s)	4IF1
	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer security and forensic computing
Paper No.	1
External Examiner(s)	Prof. J.A. Keane
Internal Examiner(s)	Prof. G. Lyons
	Dr. C. Mulvihill
Instructions:	Answer any four questions.
	All questions carry equal marks.
Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

1
An entrepreneur developing software for the healthcare sector has secured funding and is setting up in the west of Ireland. You have been retained to provide initial advice on a security profile. Discuss elements of a report you might draft for this individual, making use of the following three headings: general IP protection (8 marks), regulatory compliance (8 marks), web and wireless exposure (9 marks).

2
(a) What is your understanding of the term 'steganography'? (6 marks)
(b) Is steganography difficult to detect in your opinion? (8 marks)
(c) Outline how a simple message might be concealed in an image using a least significant bit technique, and estimate how much information could be hidden in a single 1024*1024 image using this approach (11 marks)

3 'Security is often concerned with confidentiality and integrity'
(a) Give a brief outline of two significant properties of the Bell-LaPadula model (8 marks)
(b) In the context of the Chinese wall model, explain what is meant by a 'conflict set' (8 marks)
(c) Outline your understanding of the main elements of the BMA security policy (9 marks)

4
'Cryptography may or may not be secure'
(a) Explain what is meant by the terms 'symmetric key cryptography' and 'public key cryptography' (6 marks)
(b) Discuss how an on-line trading organisation might make use of public, private, and session keys in its dealings with customers, explaining the terms 'digital certificate' and 'digital signature' in the course of your answer (9 marks)
(c) You have access to a hard drive that is apparently encrypted. Given a plain text sample with a period of six bytes, and an encrypted sample with a period of twenty four bytes, outline how you might proceed to investigate the strength of the encryption, given that you suspect that a form of linear encryption is in place (10 marks)

5
(a) Give your understanding of the term 'phishing' (7 marks)
(b) What is meant by the use of 'fast-flux services' for phishing? (8 marks)
(c) The FTC has linked phishing to identity theft. What steps would you devise in order to lessen the likelihood of your company's employees becoming victims of phishing activities? In the course of your answer, explain the term 'educational landing page' (10 marks)

6
(a) Give your understanding of the 'Daubert Criteria' for scientific evidence (7 marks)
(b) Explain what is meant by a hash function and discuss why such functions are of use in digital forensics (8 marks)
(c) Outline the steps that you would take in imaging a disk and searching it for content, explaining the terms 'dd' and 'data carving' in the course of your answer (10 marks)

7
'The jury is still out on electronic voting'
Discuss this statement in the light of the relevant German Federal Constitutional Court decision in March 2009 (25 marks)